

アンラボ・セキュリティレター

Press **Ahn**

---

2015.10 Vol.22

直感的かつシンプルな追加認証サービスの実現



## SIM カードベース追加認証サービス「AhnLab シンプル認証(仮)」リリース

# 直感的かつシンプルな追加認証サービスの実現

韓国は2013年以降、インターネットバンキングを使用する際に「公認証明書<sup>1</sup>」で本人確認した後、次のステップとして携帯のSMS（テキストメッセージ）や電話のARSシステムを通じて本人であることを再確認する「追加認証方式」が義務付けられた。今はインターネットバンキングだけでなくオンラインショッピングにも追加認証方式が適用されている。だが最近SMSやARSのセキュリティホールが相次いで発見され、新たな認証方式の必要性が高まってきた。だが新たな認証方式を適用するとなると、ユーザーに不便を強いることになりかねない上にサービス構築そのものも容易ではなく、いくつかのハードルが存在する。そこでアンラボでは新たな認証システムの利便性を高める「AhnLabシンプル認証(仮)」をリリースすることになった。プレス・アン今月号ではアンラボの新たな認証サポートソリューションを紹介する。

### 一般ユーザー：A氏

「スマートフォンからの会員登録がとても面倒です。同意項目にすべてチェックして本人確認も済ませたのに、またSMSでナンバーを受信して再入力させるし、何とか全てクリアしてやっと認証完了したのにすでに他の人が私の名義で会員登録してポイントも使用中とのこと。これはどういうことですか？」

### カード会社のセキュリティ管理者：B氏

「追加認証プロセスの適用が義務化されたのにSMSやARS方式はセキュリティ性が脆弱だと言われていました。かといってセキュリティが強化された新技術を適用しようとするれば、構築作業の手間やユーザービリティも複雑な製品が多く、お客様からのクレームは避けられません。どうしたらよいか悩みどころです。」

<sup>1</sup> 韓国の電子商取引を行う際に身元を確認し、文書偽造と改ざんや取引内容の否認防止などを目的として公認認証機関(CA)で発行する電子的情報であり、サイバー取引のための一種の印鑑証明書。インターネットで行政手続きやインターネットバンキングを利用する際に認証手段として利用する。日本の公的個人認証サービス(JPKI)と同じ位置づけ。

最初のケースは、直近放送された某TV番組の内容を再構成したものである。ユーザーが集めたポイントを使用するためには複雑な本人認証のステップを経る必要があり、何とかこの確認ステップを完了したもののすでに誰かが「私」の名義で堂々と会員登録をしてポイントまで使用していた。

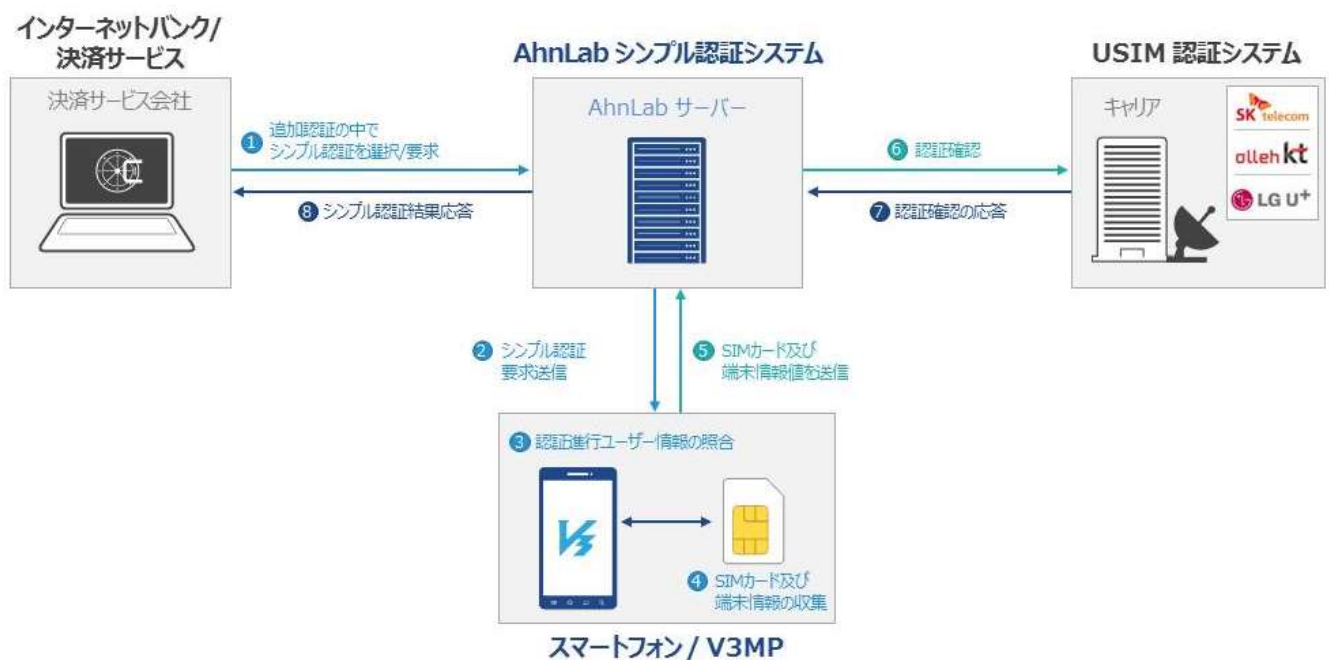
この一連の件で生じる感情の矛先が、カード会社などのサービスプロバイダに向けられるのは当然のことであろう。

だが企業側にとっても困惑は尽きない。安全な電子金融取引のために本人認証方式を適用しているが使用するには手間がかかる上、本人でなくても本人認証を行ってしまうのだ。また企業ネットワークの侵入に加え、個人使用の端末がハッキングされて発生する金融アクシデントの場合も、電子金融取引法に基づいて企業側に責任が問われるため本人認証は企業としても非常に扱いにくい事案なのだ。最近ではユーザービリティを強化した SIMカードベースの追加認証ソリューションが増えてきているが、ソリューションの構築や適用が簡単ではないことも企業を悩ませている。

### より強固なセキュリティ性はもちろん、簡単な構築も重要

追加認証プロセスの適用によるユーザーの手間や企業側の負担を解消することを目的に、アンラボでは SIMカードベースの追加認証サービス「AhnLab シンプル認証」をリリースした。アンラボは今年に入りキャリア 3社と MOU を結び、スマートフォン USIM(Universal Subscriber Identification Module)ベースでユーザー端末占有認証をベースにした新たな追加認証サービスを開発した。本製品はアンラボの強力なセキュリティモジュールと SIMカード、キャリアの端末情報を組み合わせた新たな認証サービスである。

仕組みとしては、まずオンライン決済プロセスの中で追加認証の段階でサービス会社がユーザー認証を要求する。アンラボのシンプル認証システムのサーバーで前述の要求を受信後スマートフォンの SIMカードに保存された情報と、キャリアに登録された名義および端末情報と一致するかどうかを確認する。確認完了後、認証結果値が返ってくる流れとなる。ユーザー名義で登録された端末情報と照合して本人認証を行うため、前述したケースのように他人がユーザー名義で会員登録をしたりポイントを使用することができなくなる。



[図1] AhnLab シンプル認証の動作フロー

AhnLabシンプル認証は[図1]のように「多者間相互認証方式」で構成され、情報流出の脅威を最小限に抑えながら高い信頼性を提供する。

サーバーと端末間すべてのメッセージが鍵ペアで暗号化されて1回の処理の制限時間(Time Limit)値を持つ。これによりすましによる改ざんや、特に制限時間内の改ざんが難しくなるため認証の安全性を高めることができる。また保護対象のデータに対する推測や一時パスワード作成が可能なOTP方式とは異なり、セキュリティレベルが高いSIMカードに鍵を保存・管理するためキー流出などの心配も不要だ。

強力なセキュリティを提供する一方で本製品のインストールおよび使用方法が非常に簡単である。Androidスマートフォンにインストールした金融取引専用のセキュリティソリューション「AhnLab V3 Mobile Plus」に追加機能として提供されるため、簡単なインタフェースの操作以外に別途の構築と開発作業を必要としない。アンラボのV3 Mobile Plusは韓国の主要金融機関サービスに導入されており、現在約3,700万人のスマートフォン金融取引のユーザーが利用している。このためサービスの迅速な適用が可能であることも魅力的といえるだろう。

## ワンタッチで簡単かつシンプルな追加認証

AhnLabシンプル認証は、サービス導入における手軽さだけでなくユーザービリティが最大化されたソリューションだ。強力なセキュリティ性にも関わらず、認証段階が大幅に簡素化されている。長くて複雑な個人情報を入力→認証コードの確認→直接入力までの面倒な従来の認証方式とは異なり、ワンタッチでユーザー認証が可能となる。AhnLab V3 Mobile PlusがインストールされたAndroidスマートフォン利用者であれば別途アプリをインストールすることなく、本製品を利用して追加認証できる。

ただしiPhoneユーザーはアプリストアで「AhnLabシンプル認証」アプリをインストールしてから利用できる。AhnLab V3 Mobile PlusがインストールされていないAndroidスマートフォンではios同様、まずV3 Mobile Plus2.0をインストールし、簡単な初期設定後に利用できる。



[図2] AhnLabシンプル認証画面 (Android用と iPhone用)

## クレジットカード会社でも AhnLab シンプル認証サービスに注目

韓国の主要銀行やカード会社にとって、より効果的な自己認証方式の導入が悩みの種となっている中、まず最初にサムスンカードが本製品の導入に踏み切ることに。サムスンカードは、カード業界初スマートフォンベース認証方式を自社に導入することになり、同社カードのユーザーは従来の SMS、ARS 方式の他、本製品を自己認証に選択することもできる。サムスンカードは、電子財布サービスである「mポケット」およびアプリカード登録時の本人認証手続きに適用し、徐々に本人認証が必要な様々なサービス領域に拡大していく予定だ。

アンラボは今後も、カード、銀行、証券、決済、ショッピングなど本人認証が必要な様々な領域に「AhnLab シンプル認証」を提供できるものと期待している。



<http://jp.ahnlab.com>

<http://global.ahnlab.com>

<http://www.ahnlab.com>



## アンラボとは

株式会社アンラボは、業界をリードする情報セキュリティソリューションの開発会社です。

1995年から弊社では情報セキュリティ分野におけるイノベーターとして最先端技術と高品質のサービスをご提供できるように努力を傾けてまいりました。今後もお客様のビジネス継続性をお守りし、安心できるIT環境づくりに貢献しながらセキュリティ業界の先駆者になれるよう邁進してまいります。

アンラボはデスクトップおよびサーバー、携帯電話、オンライントランザクション、ネットワークアプライアンスなど多岐にわたる総合セキュリティ製品のラインナップを揃えております。どの製品も世界トップクラスのセキュリティレベルを誇り、グローバル向けコンサルタントサービスを含む包括的なセキュリティサービスをお届け致します。

# AhnLab

〒108-0014 東京都港区芝4丁目13-2 田町フロントビル3階 | TEL: 03-6453-8315 (代)

© 2015 AhnLab, Inc. All rights reserved.